US009479935B2

(12) **United States Patent**
Ptasinski et al.

(10) **Patent No.: US 9,479,935 B2**
(45) **Date of Patent: *Oct. 25, 2016**

(54) **CONFIGURATOR FORCED CLIENT NETWORK REJOINING**

(71) Applicant: **Broadcom Corporation**, Irvine, CA (US)

(72) Inventors: **Henry Ptasinski**, San Francisco, CA (US); **Edward Carter**, Sunnyvale, CA (US); **Manoj Thawani**, San Jose, CA (US); **Manas Deb**, San Jose, CA (US); **Jeff Vadasz**, Los Altos, CA (US); **Mahesh Iyer**, Sunnyvale, CA (US)

(73) Assignee: **BROADCOM CORPORATION**, Irvine, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 5 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/586,371**

(22) Filed: **Dec. 30, 2014**

(65) **Prior Publication Data**

US 2015/0121494 A1 Apr. 30, 2015

Related U.S. Application Data

(63) Continuation of application No. 14/035,607, filed on Sep. 24, 2013, now Pat. No. 8,959,601, which is a continuation of application No. 13/190,053, filed on Jul. 25, 2011, now Pat. No. 8,572,700, which is a

(Continued)

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04W 12/06	(2009.01)
H04W 24/02	(2009.01)

(Continued)

(52) **U.S. Cl.**

CPC ***H04W 12/06*** (2013.01); ***H04L 41/0816*** (2013.01); ***H04L 63/0846*** (2013.01); ***H04L 63/12*** (2013.01); ***H04W 24/02*** (2013.01); *H04L 63/162* (2013.01); *H04W 8/22* (2013.01);

(Continued)

(58) **Field of Classification Search**

CPC ... H04W 12/06; H04W 24/02; H04W 12/10; H04W 8/245; H04W 8/22; H04W 12/12; H04L 41/0816; H04L 63/0846; H04L 63/12; H04L 63/162

USPC 726/6, 1, 7, 3, 11

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,377,814 B1 * 4/2002 Bender H04W 52/20 370/311

6,859,135 B1 * 2/2005 Elliott H04W 52/0235 340/7.32

(Continued)

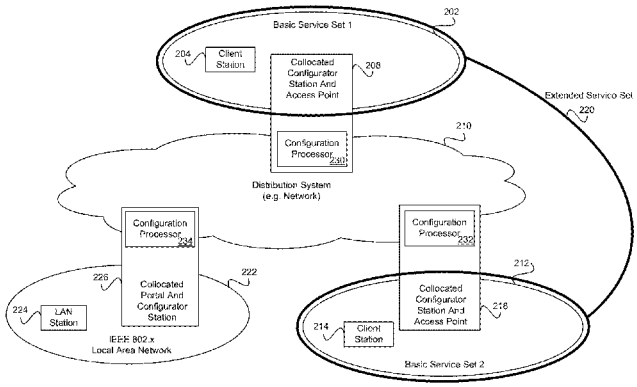
Primary Examiner — David García Cervetti

(74) *Attorney, Agent, or Firm* — Garlick & Marksion; Edward J. Marshall

(57) **ABSTRACT**

A collocated device functioning as a configurator can use short and long button activations to enter a configuration state, open a timing window, and force client devices currently joined to a network to rejoin the network. If the collocated device functioning as a configurator is unconfigured, a short (or long) button activation can initiate a configuration sequence. A short button activation on that same collocated device, once configured, can cause the device to open a configurator timing window, during which one or more devices can be provided the information necessary to securely communicate on a network. A long (or short) button activation can be used to force all currently connected client devices, or rejoin the network using a new Service Set Identifier (SSID) or passphrase.

20 Claims, 8 Drawing Sheets



Related U.S. Application Data

continuation of application No. 11/208,081, filed on Aug. 18, 2005, now Pat. No. 7,987,499.

(60) Provisional application No. 60/602,396, filed on Aug. 18, 2004, provisional application No. 60/671,120, filed on Apr. 14, 2005.

(51) **Int. Cl.**

H04L 12/24	(2006.01)
H04W 8/22	(2009.01)
H04W 8/24	(2009.01)
H04W 12/10	(2009.01)
H04W 12/12	(2009.01)

(52) **U.S. Cl.**

CPC *H04W8/245* (2013.01); *H04W 12/10* (2013.01); *H04W 12/12* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,024,218	B2 *	4/2006	Bender	H04W 52/20 455/422.1
7,103,354	B2 *	9/2006	Yamano	H04L 41/0213 455/418
7,224,704	B2 *	5/2007	Lu	H04W 8/245 370/334
7,333,460	B2 *	2/2008	Vaisanen	H04W 48/12 370/230
7,343,411	B2 *	3/2008	Cohen	H04L 63/083 709/217
7,398,550	B2 *	7/2008	Zick	H04L 63/0853 726/5
7,468,981	B2 *	12/2008	Weis	H04J 3/0661 370/394
7,567,540	B2 *	7/2009	Sakoda	H04W 48/08 370/328
7,636,331	B2 *	12/2009	Lee	H04B 7/2603 370/312
7,639,661	B2 *	12/2009	Iwami	H04W 56/0045 370/345
7,650,411	B2 *	1/2010	Cohen	H04L 63/083 709/217
7,760,680	B2 *	7/2010	Chen	H04L 12/5695 370/328
7,809,835	B2 *	10/2010	Reunamaki	H04W 84/18 455/464
7,974,191	B2 *	7/2011	Bhandari	H04L 49/90 370/208
7,987,499	B2 *	7/2011	Ptasinski	H04L 63/12 726/3
8,036,183	B2 *	10/2011	Ptasinski	H04W 8/22 370/328
8,036,639	B2 *	10/2011	Carter	H04L 63/083 380/270
8,051,463	B2 *	11/2011	Thawani	H04W 8/20 370/352
2002/0155852	A1 *	10/2002	Bender	H04W 52/20 455/522
2003/0067892	A1 *	4/2003	Beyer	H04L 45/20 370/328
2003/0185241	A1 *	10/2003	Lu	H04W 8/245 370/476
2004/0032625	A1 *	2/2004	Yamano	H04L 41/0213 358/405
2005/0043051	A1 *	2/2005	Takano	H04W 52/40 455/522
2005/0220145	A1 *	10/2005	Nishibayashi	H04W 99/00 370/474
2005/0277385	A1 *	12/2005	Daum	H04B 17/382 455/67.11
2006/0039563	A1 *	2/2006	Carter	H04L 63/083 380/270
2006/0056378	A1 *	3/2006	Sugaya	H04W 74/002 370/347
2006/0072488	A1 *	4/2006	Meier	H04L 12/1886 370/312
2006/0164969	A1 *	7/2006	Malik	H04B 7/0408 370/203
2006/0165024	A1 *	7/2006	Iwami	H04W 48/08 370/315
2007/0036096	A1 *	2/2007	Sinivaara	H04W 52/0229 370/318
2007/0217385	A1 *	9/2007	Meier	H04L 47/32 370/338
2012/0093137	A1 *	4/2012	Sakoda	H04L 47/10 370/336

* cited by examiner

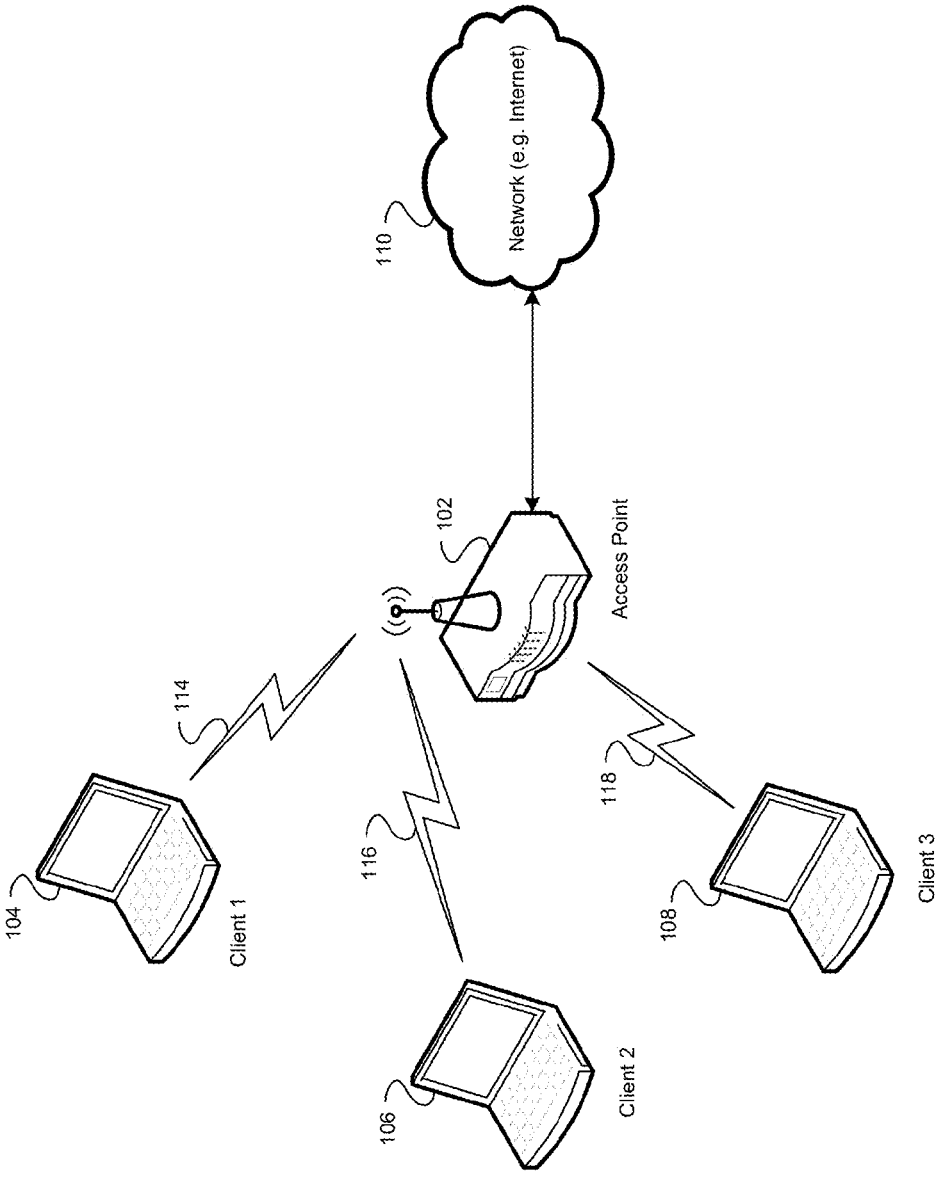

Network (e.g. Internet)
110
102
Access Point
114
116
118
104
Client 1
106
Client 2
108
Client 3

FIG. 1

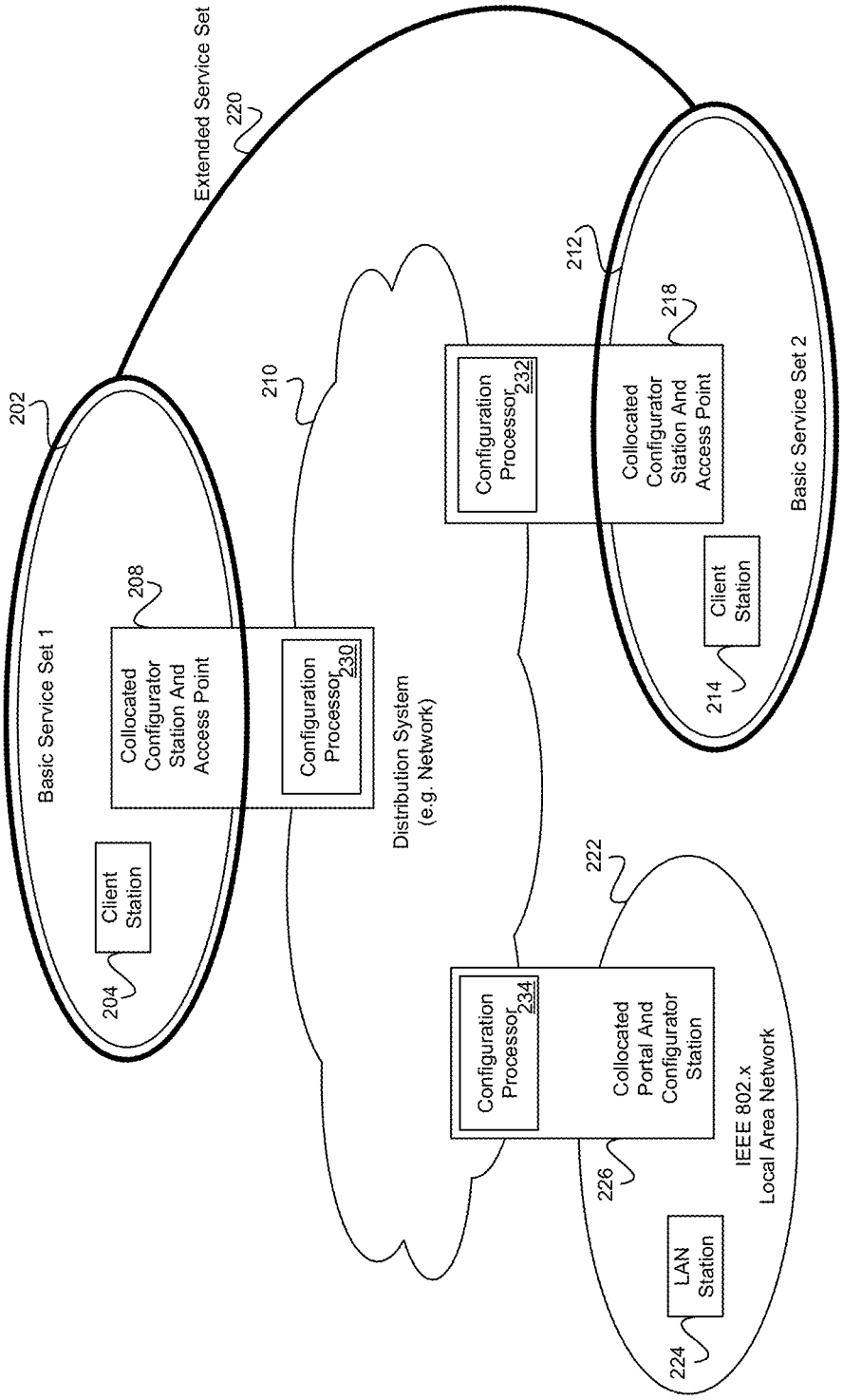

Extended Service Set
220
202
Basic Service Set 1
208
Collocated Configurator Station And Access Point
Configuration Processor 230
Client Station
204
210
Distribution System (e.g. Network)
Configuration Processor 232
212
218
Collocated Configurator Station And Access Point
Basic Service Set 2
Client Station
214
222
Configuration Processor 234
Collocated Portal And Configurator Station
IEEE 802.x Local Area Network
226
LAN Station
224

FIG. 2

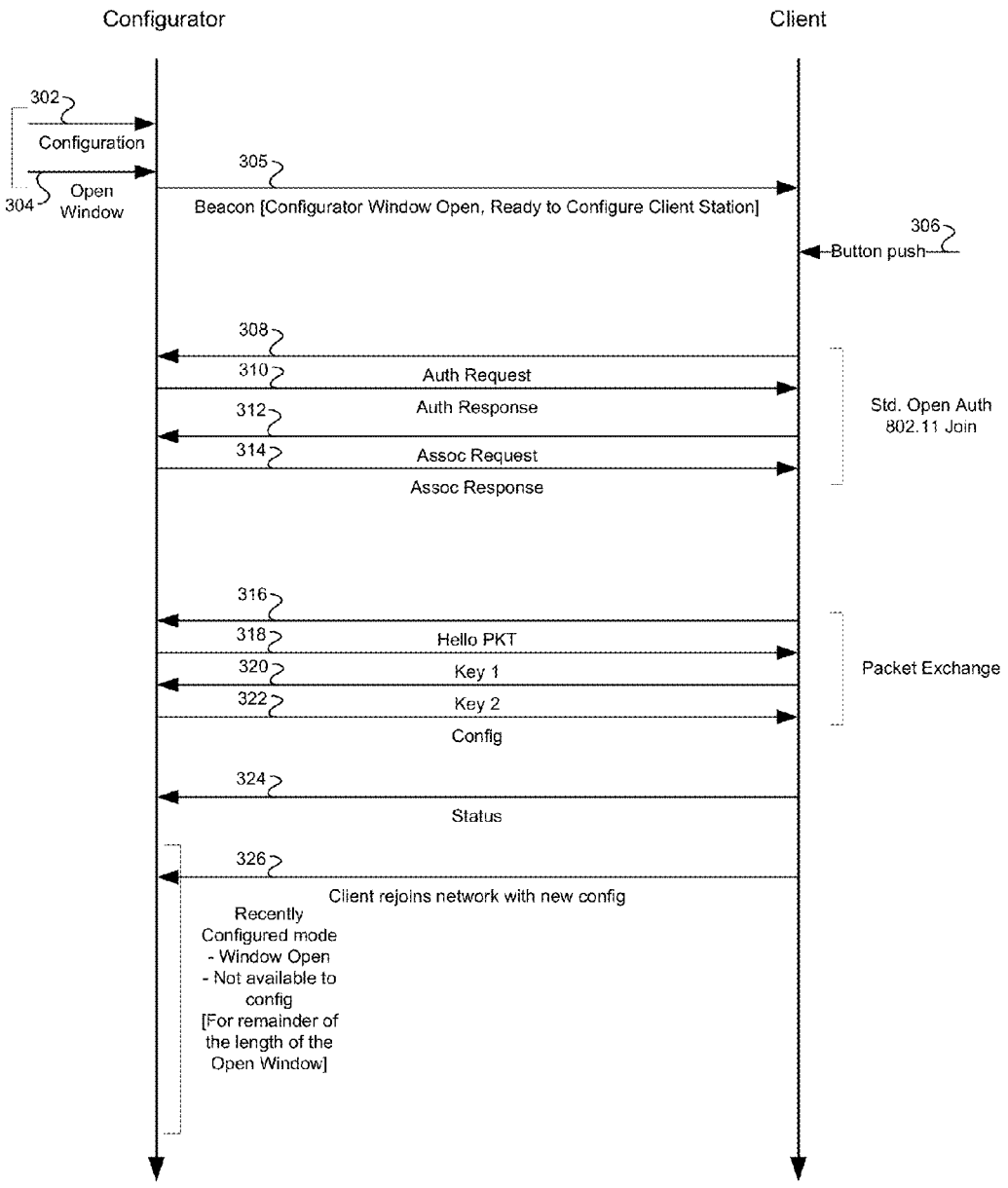

Configurator
Client
302
Configuration
304
Open Window
305
Beacon [Configurator Window Open, Ready to Configure Client Station]
306
Button push
308
310
Auth Request
312
Auth Response
314
Assoc Request
Assoc Response
Std. Open Auth 802.11 Join
316
318
Hello PKT
320
Key 1
322
Key 2
Config
Packet Exchange
324
Status
326
Client rejoins network with new config
Recently Configured mode
- Window Open
- Not available to config
[For remainder of the length of the Open Window]

FIG. 3

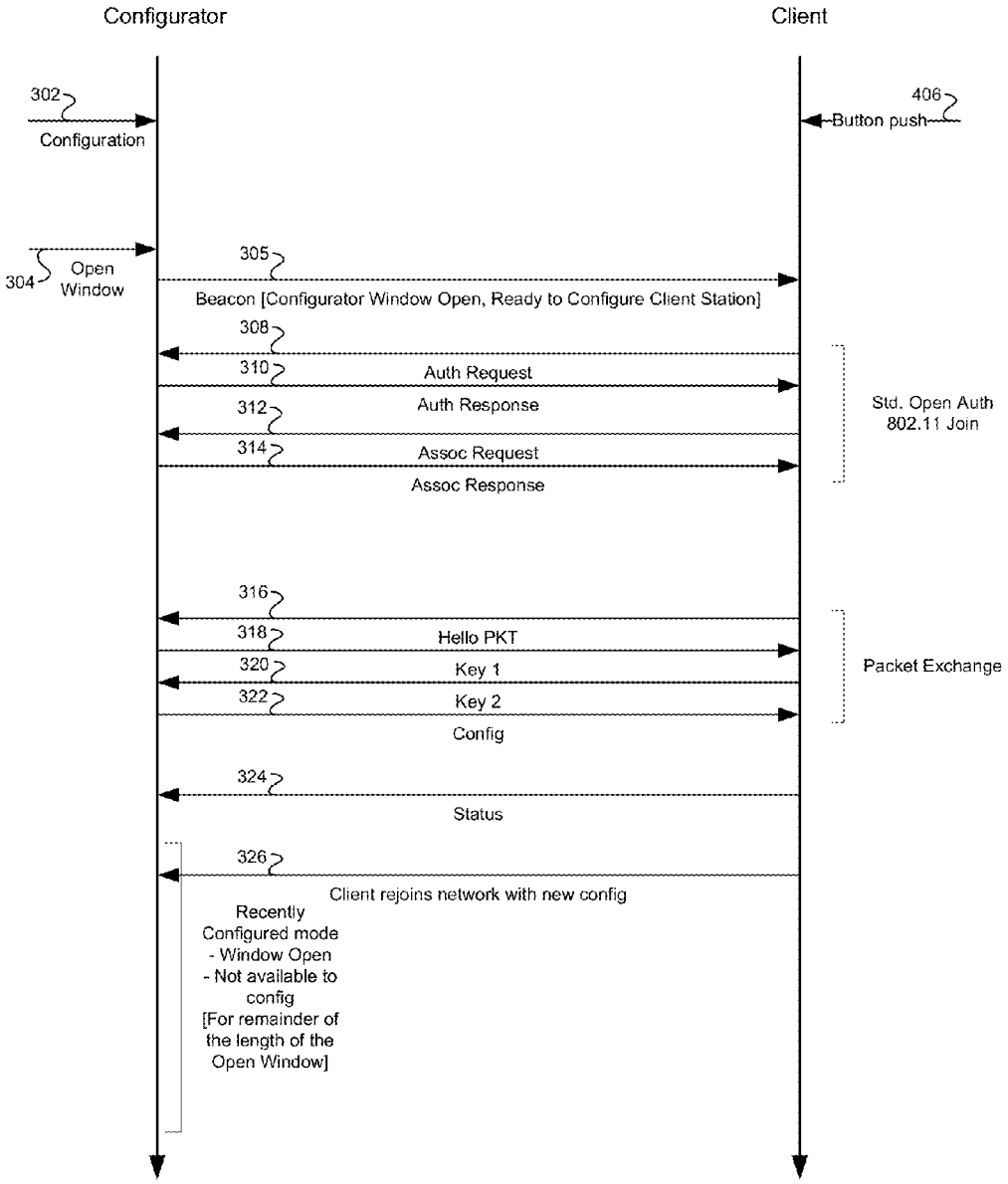

Configurator
Client
302
Configuration
406
Button push
304
Open Window
305
Beacon [Configurator Window Open, Ready to Configure Client Station]
308
310
Auth Request
312
Auth Response
314
Assoc Request
Assoc Response
Std. Open Auth 802.11 Join
316
318
Hello PKT
320
Key 1
322
Key 2
Config
Packet Exchange
324
Status
326
Client rejoins network with new config
Recently Configured mode - Window Open - Not available to config [For remainder of the length of the Open Window]

FIG. 4

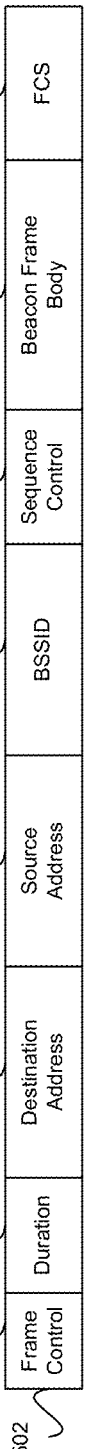

502
504
Frame Control
506
Duration
508
Destination Address
510
Source Address
512
BSSID
514
Sequence Control
516
Beacon Frame Body
518
FCS

FIG. 5a

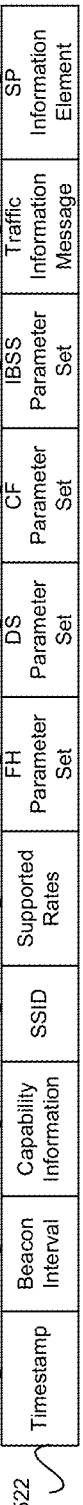

522
524
Timestamp
526
Beacon Interval
528
Capability Information
530
SSID
532
Supported Rates
534
FH Parameter Set
536
DS Parameter Set
538
CF Parameter Set
540
IBSS Parameter Set
542
Traffic Information Message
544
SP Information Element

FIG. 5b

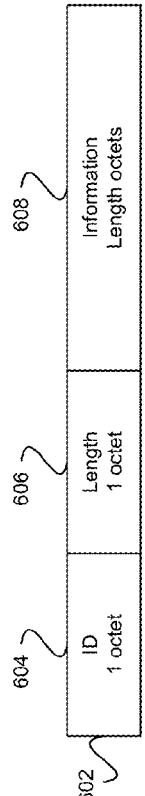


FIG. 6a

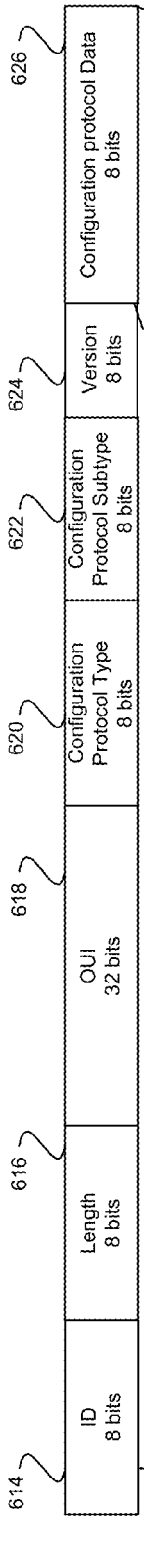


FIG. 6b

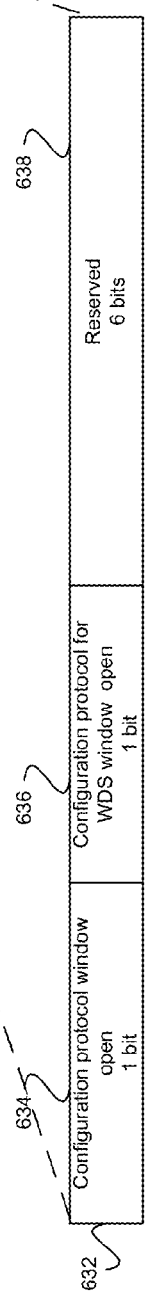


FIG. 6c

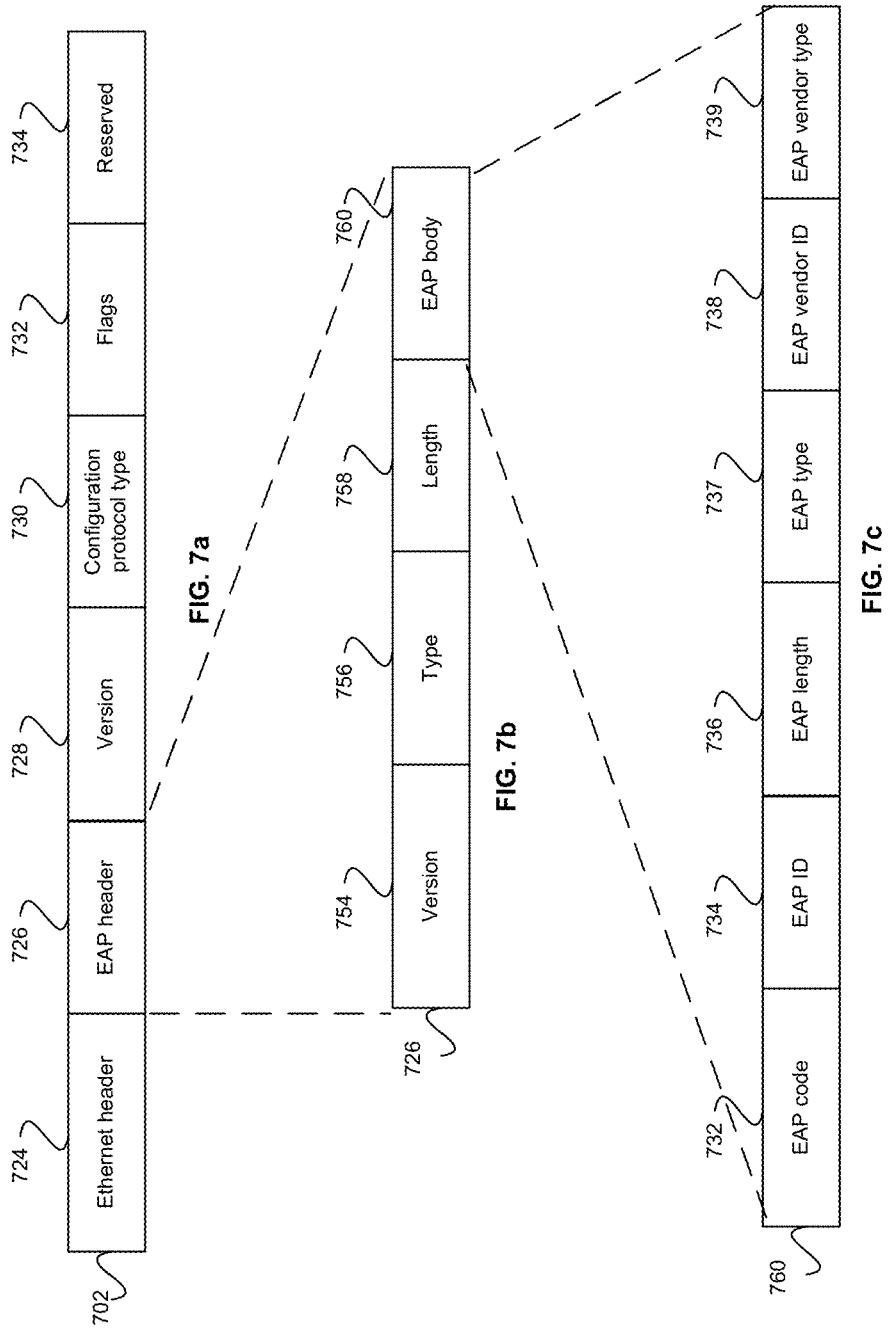


FIG. 7a

FIG. 7b

FIG. 7c

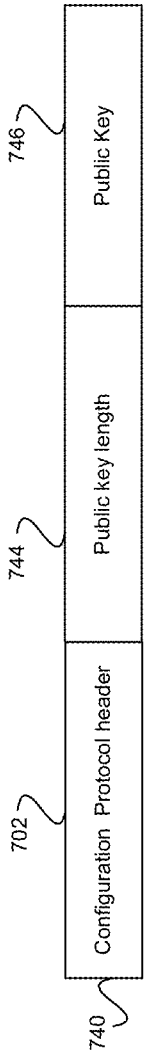

740
Configuration Protocol header
702
Public key length
744
Public Key
746

FIG. 7d

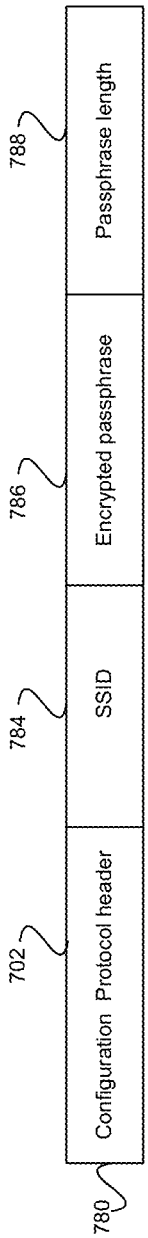

780
Configuration Protocol header
702
SSID
784
Encrypted passphrase
786
Passphrase length
788

FIG. 7e

CONFIGURATOR FORCED CLIENT NETWORK REJOINING

CROSS-REFERENCE TO RELATED APPLICATIONS/INCORPORATION BY REFERENCE

The present U.S. Utility Patent Application claims priority pursuant to 35 U.S.C. §120, as a continuation of U.S. application Ser. No. 14/035,607 entitled "Client Configuration During Timing Window" filed Sep. 24, 2013, issued as U.S. Pat. No. 8,959,601, on Feb. 17, 2015, which is a continuation of U.S. application Ser. No. 13/190,053 entitled "Method and System for Exchanging Setup Configuration Protocol Information in Beacon Frames in a WLAN" filed Jul. 25, 2011, issued as U.S. Pat. No. 8,572,700 on Oct. 29, 2013, which is a continuation of U.S. application Ser. No. 11/208,081, entitled "Method and System for Exchanging Setup Configuration Protocol Information in Beacon Frames in a WLAN," filed Aug. 18, 2005, issued as U.S. Pat. No. 7,987,499 on Jul. 26, 2011, which claims priority pursuant to 35 U.S.C. §119(e) to U.S. Provisional Patent Application No. 60/602,396 filed Aug. 18, 2004 and to U.S. Provisional Patent Application No. 60/671,120 filed Apr. 14, 2005, all of which are hereby incorporated herein by reference in heir entirety and made a part of the present U.S. Utility Patent Application for all purposes.

This application makes reference to:

U.S. application Ser. No. 11/207,302 filed Aug. 18, 2005, issued as U.S. Pat. No. 7,996,664 on Aug. 9, 2011;

U.S. application Ser. No. 11/207,262 filed Aug. 18, 2005, issued as U.S. Pat. No. 7,653,036 on Jan. 26, 2010;

U.S. application Ser. No. 11/207,658 filed Aug. 18, 2005, issued as U.S. Pat. No. 8,036,183 on Oct. 11, 2011;

U.S. application Ser. No. 11/208,310 filed Aug. 18, 2005, issued as U.S. Pat. No. 8,036,639 on Oct. 11, 2011;

U.S. application Ser. No. 11/208,275 filed Aug. 18, 2005, issued as U.S. Pat. No. 8,589,687 on Nov. 19, 2013;

U.S. application Ser. No. 11/208,346 filed Aug. 18, 2005, issued as U.S. Pat. No. 8,514,748 on Aug. 20, 2013;

U.S. application Ser. No. 11/207,661 filed Aug. 18, 2005;

U.S. application Ser. No. 11/207,301 filed Aug. 18, 2005, issued as U.S. Pat. No. 7,343,411 on Mar. 11, 2008;

U.S. application Ser. No. 11/208,284 filed Aug. 18, 2005, issued as U.S. Pat. No. 8,051,463 on Nov. 11, 2011; and

U.S. application Ser. No. 11/208,347 filed Aug. 18, 2005, issued as U.S. Pat. No. 7,930,737 on Apr. 19, 2011.

All of the above referenced applications are hereby incorporated herein by reference in their entirety and for all purposes.

FIELD OF THE INVENTION

Certain embodiments of the invention relate to wireless network communication. More specifically, certain embodiments of the invention relate to a method and system for exchanging setup configuration protocol information in beacon frames in a WLAN.

BACKGROUND OF THE INVENTION

Currently, with some conventional systems, setting up a wireless network generally requires significant interaction and technical knowledge on the part of a user setting up the network, especially when the user is configuring security options for the network. For computer savvy users, the tasks associated with setting up a wireless network may be time consuming. However, for inexperienced computer users, the tasks associated with setting up a wireless network may be more challenging and consumes significantly greater time than required by computer savvy users.

In general, 802.11-based networks require a significant amount of user interaction during the configuration process. Typically, with conventional 802.11-based networks, the user needs to configure a station (STA) to associate to an access point (AP), which may require a number of settings to be selected on the STA, and some knowledge of the default configuration of the AP. The user may then access an HTML-based menu on the new AP in order to set various configuration parameters, many of which are difficult for novice and for intermediate users to understand and set correctly. New APs generally start with a configuration that provides no network security, and which utilize a default network name (SSID) that is selected by the manufacturer such as, for example, "Manufacturer Name", "Default", or "wireless". With the proliferation of 802.11 networks, users often experience confusion and network problems when their new AP uses the same SSID as a neighboring AP. In order to facilitate communication between access points and access devices such as wireless STAs, various protocols are required. While the 802.11 WLAN standard provides a basis for implementing WLAN, it lacks various features that may be utilized to address the confusion, network problems and issues that users face when, for example, their new AP uses the same SSID as a neighboring AP.

Further limitations and disadvantages of conventional and traditional approaches will become apparent to one of skill in the art, through comparison of such systems with some aspects of the present invention as set forth in the remainder of the present application with reference to the drawings.

BRIEF SUMMARY OF THE INVENTION

A method and system for exchanging setup configuration protocol information in beacon frames in a WLAN, substantially as shown in and/or described in connection with at least one of the figures, as set forth more completely in the claims.

These and other advantages, aspects and novel features of the present invention, as well as details of an illustrated embodiment thereof, will be more fully understood from the following description and drawings.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

FIG. **1** is a block diagram of an exemplary wireless network, which may be utilized in connection with an embodiment of the invention.

FIG. **2** is a block diagram of an exemplary system for wireless data communications comprising an ESS with collocation of configurators and access points (AP), in accordance with an embodiment of the invention.

FIG. **3** is a diagram illustrating exemplary message exchanges based on a configuration protocol and initiated at the configurator, in accordance with an embodiment of the invention.

FIG. **4** is a diagram illustrating exemplary message exchanges based on a configuration protocol and initiated at the client station, in accordance with an embodiment of the invention.

FIG. **5***a* is a block diagram for an exemplary beacon frame format, in accordance with an embodiment of the invention.

FIG. **5***b* is a block diagram for an exemplary beacon frame body format, in accordance with an embodiment of the invention.

FIG. **6***a* is a block diagram for an exemplary IEEE 802.11 information element format, in accordance with an embodiment of the invention.

FIG. **6***b* is a diagram of an exemplary configuration protocol information element, in accordance with an embodiment of the invention.

FIG. **6***c* is a diagram of an exemplary configuration protocol data field format, in accordance with an embodiment of the invention.

FIG. **7***a* is a diagram of an exemplary configuration protocol packet header format, in accordance with an embodiment of the invention.

FIG. **7***b* is a diagram of an exemplary EAP header message format for a configuration protocol, in accordance with an embodiment of the invention.

FIG. **7***c* is a diagram of an exemplary EAP header body format for a configuration protocol, in accordance with an embodiment of the invention.

FIG. **7***d* is a diagram illustrating an exemplary configuration protocol packet type key format, in accordance with an embodiment of the invention.

FIG. **7***e* is a diagram illustrating an exemplary configuration protocol packet type info format, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Certain aspects of a method for enabling exchange of information in a secure communication system may comprise configuring at least one 802.11 client station via authentication enablement information comprising data that specifies a time period during which configuration is allowed. The data that specifies a time period during which configuration is allowed may comprise a configuration window open field, which indicates a period when a configuration setup window is open. At least one client station may be configured via the authentication enablement information comprising recently configured data, which indicates whether at least one configurator has configured at least one other client station within the time period during which the configuration is allowed.

FIG. **1** is a block diagram of an exemplary wireless network, which may be utilized in connection with an embodiment of the invention. Referring to FIG. **1**, there is shown an access point (AP) **102**, and a plurality of client stations (STA) **104**, **106**, and **108**, a plurality of RF channels **114**, **116**, and **118**, and a network **110**. The AP **102** may be utilized as a configurator. The STAs **104**, **106**, and **108** may be wireless terminals such as a PC, a laptop, or a PDA with integrated or plug-in 801.11 capabilities. For example, the PC may utilize a wireless NIC card and the laptop or PDA may comprise integrated 801.11 capabilities. The network **110** may be a private or public network, for example, a service provider or the Internet.

In operation, in instances where the STAs **104**, **106**, and **108** are configured, they may communicate with the AP **102** via corresponding secure RF channels **114**, **116**, and **118**, respectively. The AP **102** may communicate information received from a configured STA **104**, **106**, or **108** via the Internet **110**. In instances where the STAs **104**, **106**, or **108** are unconfigured, they may communicate with the AP **102** functioning as a configurator to request configuration information. The AP **102** functioning as a configurator may configure a requesting STA **104**, **106**, or **108** via a corresponding RF channel **114**, **116**, or **118**.

FIG. **2** is a block diagram of an exemplary system for wireless data communications comprising an extended service set (ESS) with collocation of configurators and access points (AP), in accordance with an embodiment of the invention. With reference to FIG. **2** there is shown a distribution system (DS) **210**, an extended service set (ESS) **220**, and an IEEE 802 LAN **222**. The ESS **220** may comprise a first basic service set (BSS) **202**, and may include a second BSS **212**, and may also include additional BSSs. The first BSS **202** may comprise a client station **204**, and a collocated configurator station and access point **208**. The collocated configurator station and access point **218** may comprise a configuration processor **230**. The second BSS **212** may comprise a client station **214**, and a collocated configurator station and access point **218**. The collocated configurator station and access point **218** may comprise a configuration processor **232**. The IEEE 802 LAN **222** may comprise a LAN station **224**, and a collocated configurator station and access point **226**. The collocated configurator station and access point **226** may comprise a configuration processor **234**.

The collocated configurator station and access point **208** may be adapted to function as an access point or as a configurator station. Throughout this application, for simplicity, collocated configurator station and access point **208** may be referred to as collocated device **208**. Accordingly, the collocated device **208** functioning as an access point refers to the collocated configurator station and access point **208** functioning as an access point. Additionally, the collocated device **208** functioning as a configurator refers to the collocated configurator station and access point **208** functioning as a configurator. The plurality of configuration processors, for example, configuration processor **230**, **232** and **234** may comprise suitable logic, circuitry and/or code that may be adapted to use authentication enablement information comprising data that specifies a time period during which configuration of at least one 802.11 client station, for example, client station **104** may be allowed.

A BSS **202** may comprise a plurality of proximately located stations that may communicate wirelessly, via a wireless medium. A BSS **202** that is also associated with an ESS **220** may be referred to as an infrastructure BSS. The wireless medium may comprise an RF channel. The ESS **220**, comprising a plurality of BSSs, BSS **202** and BSS **212**, for example, may be identified by a unique service set identifier (SSID). The portal **226** may also be a member in the ESS **220**. Stations **204** and **214**, associated with an ESS **220**, may communicate via a wireless medium and/or via a distribution system medium, for example the DS **210**. The DS **210** may comprise a distribution system medium that further comprises a wired medium and/or a wireless medium. A wired medium may comprise a physical communications channel that enables STA **204** to transmit information via a plurality of communications technologies, for example electrical or optical signals. In an IEEE 802.11 WLAN, the collocated configurator station and access point **208** or collocated configurator station and access point **218** may comprise the functionality of an AP and the functionality of a configurator. In an IEEE 802.11 WLAN, an AP may comprise the functionality of a station.

The collocated device **208** functioning as an AP, may enable STA **204** to transmit information via the DS **210**. Portal **226** may enable a LAN station **224**, which is located in a traditional IEEE 802 LAN, to communicate with an IEEE 802.11 STA **204**, via the DS **210**. A traditional IEEE

802 LAN may comprise a wired medium. An IEEE 802 LAN **222** may not comprise an IEEE 802.11 WLAN, for example BSS **202**. The DS **210** may utilize media access control (MAC) layer IEEE 802 addressing and/or network layer addressing. If the DS **210** utilizes MAC layer IEEE 802 addressing, the collocated device **208**, functioning as an AP, collocated configurator station and access point **218** functioning as an AP, and/or the portal **226** may comprise Ethernet switching device functionality. If the DS **210** utilizes network layer addressing, the collocated device **208**, functioning as an AP, collocated configurator station and access point **218** functioning as an AP, and/or the portal **226** may comprise router functionality.

The collocated device **208** functioning as a configurator may configure a STA **204**, thereby enabling the STA **204** to communicate wirelessly in a secure IEEE 802.11 network that utilizes encryption. The collocated device **208** functioning as a configurator, may configure a STA **204** by communicating information to the STA **204** comprising an SSID and an encryption key. The encryption key may also be referred to as a passphrase. A configured STA **204** may be authorized to utilize an IEEE 802.11 network based on the received configuration information from the collocated device **208** functioning as a configurator. A process by which the STA **204** is authenticated may comprise configuration of the STA **204**. Various embodiments of the invention comprise a method and a system for configuring the STA **204** while requiring less manual intervention from a user than is the case with some conventional methods and/or systems for configuring the STA **204**.

A non-AP station, for example, the client station **204** within the BSS **202** may subsequently form an association with the collocated device **208** functioning as an AP. The STA **204** may communicate an association request to the collocated device **208** functioning as an AP, based on the SSID that was received by the STA **204** during configuration. The collocated device **208** functioning as an AP, may communicate an association response to the STA **204** to indicate to the STA **204** the result of the association request. By associating with the collocated device **208** functioning as an AP, the station **204** may become a member of BSS **202**. Furthermore, by obtaining membership in BSS **202**, the STA **204** may become authorized to engage in secure wireless communication with other client stations in the ESS **220**. Similarly, non-AP client station **214** within a BSS **212** may form an association with the collocated configurator station and access point **218** functioning as an AP, enabling the STA **214** to become a member of BSS **212**.

Subsequent to the formation of an association between the client station **204** and the collocated device **208** functioning as an AP, the collocated device **208** functioning as an AP, may communicate accessibility information about the client station **204** to other APs associated with the ESS **220**, such as the collocated configurator station and access point **218** functioning as an AP, and portals such as the portal **226**. In turn, the collocated configurator station and access point **218** functioning as an AP, may communicate accessibility information about the client station **204** to stations in BSS **212**. The portal **226**, such as for example an Ethernet switch or other device in a LAN, may communicate reachability information about the client station **204** to stations in LAN **222**, such as LAN station **224**. The communication of reachability information about the client station **204** may enable stations that are not associated in BSS **202**, but are associated in ESS **220**, to communicate with the client station **204**.

The DS **210** may provide an infrastructure that enables a client station **204** in one BSS **202**, which has been authenticated and configured in accordance with various embodiments of the invention, to engage in a secure wireless communication with a client station **214** in another BSS **212**. The DS **210** may also enable a client station **204** in one BSS **202** to communicate with a LAN station **224** in a non-802.11 LAN **222**, such as a wired LAN. The collocated device **208**, functioning as an AP, collocated configurator station and access point **218** functioning as an AP, or portal **226** may provide a facility by which a station in a BSS **202**, BSS **212**, or LAN **222** may communicate information via the DS **210**. The client station **204** in BSS **202** may communicate information to a client station **214** in BSS **212** by transmitting the information to collocated device **208** functioning as an AP. The collocated device **208** functioning as an AP may transmit the information via the DS **210** to the collocated configurator station and access point **218** functioning as an AP, which, in turn, may transmit the information to station **214** in BSS **212**. The client station **204** may communicate information to a LAN station **224** in LAN **222** by transmitting the information to collocated device **208** functioning as an AP. The collocated device **208** functioning as an AP may transmit the information via the DS **210** to the portal **226**, which, in turn, may transmit the information to the LAN station **224** in LAN **222**.

FIG. **3** is a diagram illustrating exemplary message exchanges based on a configuration protocol and initiated at the configurator, in accordance with an embodiment of the invention. FIG. **3** presents an exemplary exchange of messages between the collocated device **208** (FIG. **2**) functioning as a configurator, and the client station **204**, based on a configuration protocol. In step **302**, the collocated device **208** functioning as a configurator, may be configured. A collocated device **208** functioning as a configurator, which is not configured to supply configuration information to a requesting client station **204** during authentication may be referred to as an unconfigured collocated device **208** functioning as a configurator. In an unconfigured collocated device **208** functioning as a configurator, activation of a button located thereon for a specified time duration may initiate step **302**.

The time duration for which the button is activated may correspond to, for example, a "short" button activation. In instances where the collocated device **208** functions as a configurator, configuration may comprise entering an SSID, and/or entering a passphrase. The SSID and/or passphrase that is entered and/or generated during the configuration may subsequently be utilized when configuring client stations **204**. If a passphrase is not entered, the configurator may be adapted to generate one, which may subsequently be utilized to configure client stations **204**. The entered and/or generated configuration information may be stored in non-volatile memory, and/or in a storage device at the collocated device **208**, for example. When the collocated device **208** functions as a configurator, it may retrieve the configuration information from the non-volatile memory and/or storage device and use it to configure client stations **204**.

In a configured collocated device **208**, functioning as a configurator, activation of the button thereon for a specific time duration may result in step **302** being bypassed, and step **304** initiated. The specific time duration for which the button is activated may correspond to, for example, a short button activation. In step **304**, a configurator timing window may be opened at the collocated device **208** functioning as a configurator. The opening of the configurator timing window may correspond to the start of a time duration

during which a client station **204** may be configured by the collocated device **208** functioning as a configurator. The time during which the configurator timing window remains open subsequent to a short button activation may be configured at the collocated device **208** functioning as a configurator.

In step **305**, at a time instant subsequent to the opening of the configurator timing window in step **304**, the collocated device **208** functioning as an AP, may transmit IEEE 802.11 beacon frames comprising authentication enablement information, in accordance with an embodiment of the invention. The authentication enablement information may comprise data that indicates when the configurator timing window is open, and that the collocated device **208** functioning as a configurator is ready to configure a client station **204**. In one embodiment of the invention, the authentication enablement information may comprise a flag field, window_open, which may be set to a Boolean value to indicate whether the configurator timing window is open or closed. A logical value window_open=TRUE, or a numerical value window_open=1 may indicate that the configurator timing window is open, for example. A logical value window_open=FALSE, or a numerical value window_open=0 may indicate that the configurator timing window is closed, for example. The authentication enablement information may comprise a flag field, recently_cfg, which may be set to a Boolean value to indicate whether the collocated device **208** functioning as a configurator, is ready to configure a client station **204**. A logical value recently_cfg=FALSE, or a numerical value recently_cfg=0 may indicate that the collocated device **208** functioning as a configurator, is ready to configure a client station **204**, for example. A logical value recently_cfg=TRUE, or a numerical value recently_cfg=1 may indicate that the collocated device **208** functioning as a configurator, has already configured a client station **204** during the current configurator timing window open time interval and is not ready to configure a client station **204**, for example.

At a time instant when a configurator timing window is opened, a subsequent first beacon message, associated with the step **305**, transmitted by the collocated device **208** functioning as a configurator. The message, associated with the step **305**, may comprise flags window_open=TRUE, indicating that the configurator timing window is open, and recently_cfg=FALSE, indicating that the collocated device **208** functioning as a configurator, is ready to configure a client station **204**. Beacon frames transmitted by the collocated device **208** functioning as an AP, at instants in time during which the configurator timing window is not open may not comprise authentication enablement information. In step **305**, these beacon frames may be received by a client station **204**.

In a client station **204**, activation of the button, located at a client station **204** may initiate step **306**. In step **306**, a client timing window may be opened at the client station **204**. The opening of the client timing window may correspond to the start of a time duration in which a client station **204** may request to be configured by the collocated device **208** functioning as a configurator. The client station **204** may also start a discovery protocol. The discovery protocol comprises a process by which a client station **204** may locate a collocated device **208** functioning as a configurator, with which to initiate an authentication exchange. The client station **204** may scan beacon frames received from one or more collocated devices **208** functioning as either a configurator or an access point. A beacon frame collocated device **208** functioning as a configurator may comprise authentication enablement information. Subsequent to the opening of the client timing window, the client station **204** may communicate authentication response information to the collocated device **208** functioning as a configurator, via one or more messages associated with the steps **308**, **312**, **316**, **320** and **324**. The client station **204** may communicate the one or more messages, associated with the steps **308**, **312**, **316**, **320** and **324**, comprising authentication response information based on authentication enablement information contained in the transmitted beacon frame during a time interval in which the configurator timing window was open.

A button located at either the collocated device **208** functioning as a configurator, or the client station **204**, may comprise a hardware button, for example a physical button, and/or a software enabled button, for example, a glyph or icon that is displayed in a user interface.

Steps **308**, **310**, **312**, and **314** may comprise message exchanges based on IEEE 802.11 comprising an open authentication and join of a basic service set (BSS) as defined in IEEE 802.11. The BSS utilized during open authentication may utilize a different SSID than that utilized by the infrastructure BSS **202**. In step **308**, an authentication request message may be sent by the client station **204**, to the collocated device **208** functioning as a configurator. In step **310**, the collocated device **208** functioning as a configurator, may send an authentication response message to the client station **204**. In step **312**, the client station **204** may send an association request message, associated with the step **312**, to the collocated device **208** functioning as a configurator. In step **314**, the collocated device **208** functioning as a configurator, may send an association response message, associated with the step **314**, to the client station **204**.

Steps **316**, **318**, **320**, and **322** may comprise a packet exchange based on a configuration protocol, in accordance with various embodiments of the invention. The packet exchange may utilize, but may not be limited to, the Diffie-Hellman (DH) protocol. In step **316**, the client station **204** may communicate a hello packet to the collocated device **208** functioning as a configurator. The hello packet, associated with the step **316**, may indicate to the collocated device **208** functioning as a configurator, that the client station **204** is ready to be configured. In step **318**, the collocated device **208** functioning as a configurator, may communicate a key**1** message to the client station **204**. The key**1** message, associated with the step **318**, may comprise a configurator key. In step **320**, the client station **204** may communicate a key**2** message to the collocated device **208** functioning as a configurator. The key**2** message, associated with the step **320**, may comprise a client key.

In step **322**, the collocated device **208** functioning as a configurator, may communicate a configuration message to the client station **204**. The configuration message, associated with the step **322**, may comprise configuration information that may be utilized to authenticate a client station **204**. The configuration information communicated in the configuration message, associated with the step **322**, may be encrypted based on the configurator key and/or the client key. In step **324**, the client station **204** may communicate a status message to the collocated device **208** functioning as a configurator. The status message **324** may be sent subsequent to decryption of at least a portion of the configuration message **322**. The client station **204** may utilize the configurator key and/or the client key to decrypt at least a portion of the configuration message, associated with the step **322** that was previously encrypted by the collocated device **208** functioning as a configurator. The status message, associated with the step **324**, may indicate whether the

client station **204** was successfully configured during the packet exchange. If the client station was successfully configured, the status message, associated with the step **324**, may indicate success. The collocated device **208** functioning as a configurator, may store authentication information about the configured client **204** in persistent memory. Persistent memory may comprise any of a plurality of device storage technologies that may be utilized to maintain information about the configured client station **204** until action is taken to release the stored information from persistent memory. These actions may comprise manual intervention at the collocated device **208** functioning as a configurator, by a user, or automatic intervention by a software process executing at the configurator.

In step **326**, the client station **204** may rejoin the WLAN based on the received configuration information. The steps performed during the rejoin, associated with the step **326**, may be substantially as defined in IEEE 802.11. The rejoin, associated with the step **326**, may occur via a secure RF channel that utilizes the received configuration information in step **322**. For example, the rejoin, associated with the step **326**, may utilize the SSID that was received by the client station during the packet exchange. Subsequent to configuration of the client station **204**, the collocated device **208** functioning as a configurator, may not be available to configure another client station **106** during the current configurator registration window time interval. Beacon frames may be transmitted by the collocated device **208** functioning as an AP, subsequent to the configuration of the client station **204**. These beacon frames may comprise information that indicates that the configurator timing window is closed, and that the collocated device **208** functioning as a configurator, has already configured a client station **204** during the current configurator timing window open time duration. This may indicate to a subsequent client station **204** that receives the beacon frames that the collocated device **208** functioning as a configurator, is not currently ready to configure a client station **204**.

In various embodiments of the invention, the packet exchange, comprising the steps **316**, **318**, **320**, **322** and **324**, may be performed by a collocated device **208** functioning as a configurator, and a client station **204** that communicate wirelessly, via a wireless medium. The collocated device **208** functioning as a configurator, and client station **204** may also communicate during the packet exchange via a wired medium, for example, via an Ethernet LAN **222**. If the collocated device **208** functioning as a configurator, receives a packet, for example an authentication request, associated with the step **308**, from the client station **204**, via a wireless medium, subsequent packet exchanges between the collocated device **208** functioning as a configurator, and client station **204** may be communicated wirelessly. If the collocated device **208** functioning as a configurator receives a packet from the client station **204**, via a wired medium, subsequent packet exchanges between the collocated device **208** functioning as a configurator, and client station **204** may be communicated via a wired medium. The received packet may be, for example, a hello packet, associated with the step **316**.

In operation, if the time duration for button activation at the collocated device **208** functioning as a configurator, corresponds to a "long" button activation, the collocated device **208** functioning as a configurator, may generate a new SSID and/or passphrase. The new SSID and/or passphrase may replace an SSID and/or passphrase that was stored in the collocated device **208** functioning as a configurator, as configuration information prior to the long button activation. For either a configured, or unconfigured collocated device **208** functioning as a configurator, a long button activation may initiate step **302**. Subsequent to a long button activation, the configurator may also release, from persistent memory, configuration information pertaining to previously configured client stations **204**. As a consequence, previously configured client stations **204** may lose the ability to engage in secure wireless communications via the BSS **202** or ESS **220**. The client stations **204** may be required to repeat the process of authentication with a collocated device **208** functioning as a configurator, to regain the ability to engage in secure wireless communications via the BSS **202** or ESS **220**.

The exchange of authentication enablement information, authentication response information and configuration information in messages associated with the steps **305**, **308**, **310**, **312**, **314**, **316**, **318**, **320**, **322** and **324**, between a collocated device **208** functioning as a configurator, and a client station **204**, may occur within a time duration in which the configurator timing window is open. The configurator timing window is closed after a time interval corresponding to a configurator timing window open duration lapses or ends. The exchange of authentication enablement information, authentication response information and configuration information, in messages associated with the steps **305**, **308**, **310**, **312**, **314**, **316**, **318**, **320**, **322** and **324**, between a collocated device **208** functioning as a configurator, and a client station **204**, may occur within a time duration in which the client timing window is open. After a time interval corresponding to a client timing window open duration lapses, the client timing window is closed.

FIG. **4** is a diagram illustrating exemplary message exchanges based on a configuration protocol and initiated at the client station, in accordance with an embodiment of the invention. FIG. **4** is substantially as described in FIG. **3** with the exception that the button activation occurs at the client station **204**, to open the client timing window, at a time instant prior to a time instant at which the button activation occurs at the collocated device **208** functioning as a configurator, to open the configurator timing window. Subsequent to the button activation to open the client timing window, associated with the step **406**, at the client station **204**, the client station **204** may wait to receive a beacon frame, associated with the step **305**. The beacon frame, associated with the step **305**, may comprise authentication enablement information from the collocated device **208** functioning as an AP, prior to proceeding with step **308**. If the client station **204** had previously received, and stored, a beacon frame comprising authentication enablement information, the client station **204** may communicate an authentication request message **308** to a collocated device **208** functioning as a configurator, that transmitted the previously received beacon frame to the client station **204**. The client station **204** may not wait to receive a beacon frame, associated with the step **305**, that was transmitted by a collocated device **208** functioning as a configurator, subsequent to the button activation, associated with the step **406**, at the client station **204**. Subsequent message exchanges in FIG. **4** are substantially as described for FIG. **3**.

FIG. **5***a* is a diagram of an exemplary beacon frame format, in accordance with an embodiment of the invention. With reference to FIG. **5***a* there is shown a beacon frame format **502** with a time period, Tf equal to 10 ms. The beacon frame **502** may comprise a frame control field **504**, a duration field **506**, a destination address field **508**, a source address field **510**, a BSSID field **512**, a sequence control field **514**, a beacon frame body **516**, and a frame check

sequence (FCS) **518**. The format of the beacon frame may be based on specifications contained in IEEE standard 802.11.

The frame control field **504** may comprise information that identifies the frame as being a beacon frame. The duration field **506** may comprise information indicating the amount of time that is to be allocated for transmitting the beacon frame **502** and for receiving an acknowledgement of transmission. The destination address field **508** may comprise information identifying an address of one or more stations, such as, for example, client station **204**, that are intended to receive the beacon frame **502**. The source address field **510** may comprise information identifying the address of the station that transmitted the beacon frame **502**. The BSSID field **512** may comprise information identifying the address of an AP that is a current member of the basic service set (BSS), such as, for example BSS **102**. The sequence control field **514** may be utilized to identify a beacon frame that may be a segment within a larger protocol data unit (PDU). The beacon frame body **516** may comprise information that is specific to a beacon frame. The frame check sequence (FCS) field **518** may be utilized to detect errors in a received beacon frame **502**.

In operation, the beacon frame **502** may be communicated by an AP, such as, for example, AP **108**, in a BSS, such as, for example, BSS **102**. The beacon frame may enable stations within a BSS to locate an AP within the ESS. A station that is not a current member of the BSS may establish an association with the AP based on the BSSID field.

FIG. **5***b* is a diagram of an exemplary beacon frame body format, in accordance with an embodiment of the invention. With reference to FIG. **5***b*, there is shown a beacon frame body format **522**. The beacon frame body format **522** may comprise a timestamp field **524**, a beacon interval field **526**, a capability information field **528**, a SSID field **530**, a supported rates field **532**, a frequency hopping (FH) parameter set field **534**, a direct sequence spread spectrum parameter set field **536**, a contention free (CF) parameter set field **538**, an independent BSS (IBSS) parameter set field **540**, a traffic information message field **542**, and a setup configuration protocol (SP) information element (IE) field **544**.

The timestamp field **524** may indicate a time at which the beacon frame was transmitted. The beacon interval field **526** may indicate the amount of time that may transpire between beacon frame transmissions. The capability information field **528** may be used to communicate capabilities related to a station, such as, for example, client station **104**, that transmits the beacon frame. The SSID field **530** may identify ESS membership information of the station, such as, for example, client station **104**, transmitting the beacon. The supported rates field **532** may indicate data rates that may be supported by the station that transmitted the beacon frame. The FH parameter set field **534** may comprise information about stations that utilize frequency hopping. The DH parameter set field **536** may comprise information about stations that utilize direct sequence spread spectrum. The CF parameter set field **538** may comprise information about APs, such as, for example, AP **108**, that support contention free polling of stations in a BSS such as, for example, BSS **202**. The IBSS parameter set **540** may comprise information about stations that are members of an IBSS that do not comprise an AP and do not access stations outside of the BSS via a DS such as, for example, DS **110**. The SP IE field **544** may comprise authorization enablement information that is utilized by a configuration protocol.

In operation, a configurator, such as, for example, AP **102** functioning as a AP **102** functioning as a configurator station **102**, may transmit a beacon frame comprising the SP information element field **544**. A station within a BSS may identify a configurator based on the source address field **510** of the beacon frame, and based upon the presence of a SP information element **544** in the beacon frame body **516**. The SP information element may comprise information that is not specified in IEEE standard 802.11. Ethernet frames that comprise the SP information element may be identified based on the Ethertype field in the Ethernet frame header, where the Ethernet frame header may be as specified in IEEE 802.

FIG. **6***a* is a diagram of an exemplary IEEE 802.11 information element format, in accordance with an embodiment of the invention. With reference to FIG. **6***a*, there is shown an IEEE 802.11 information element (IE) **602**. The IEEE 802.11 IE **602** may comprise an identifier field (ID) **604**, a length field **606**, and an information field **608**. The ID field **604** may comprise 1 octet of binary information, for example. The length field **606** may comprise 1 octet of binary information, for example. The information field **608** may comprise a plurality of octets of a number specified in the length field **606**.

FIG. **6***b* is a diagram of an exemplary configuration protocol information element, in accordance with an embodiment of the invention. With reference to FIG. **6***b*, there is shown a setup configuration protocol (SP) IE **612**. The SP IE **612** may comprise an ID field **614**, a length field **616**, an organizational unique identifier (OUI) field **618**, a configuration protocol type field **620**, a configuration protocol subtype field **622**, a version field **624** and a data field **626**. The format of the SP IE **612** may be based on the IEEE 802.11 IE **602**. The ID field **614** may comprise 8 bits of binary information, for example, and may comprise a value suitable for uniquely identifying the information element as being utilized for setup. The length field **616** may comprise 8 bits of binary information, for example. The OUI field **618** may comprise 24 bits of binary information, for example, and may comprise a value suitable for unique identification.

When the configuration protocol window is opened by the configurator, for example, the AP **102** functioning as a configurator, the AP **102** may indicate this event to the other stations connected to the ESS, for example, ESS **220** by broadcasting this information in beacon frames **305** and probe response information elements. Alternatively, the ID field **614** may comprise a value suitable for identifying the information element as a category of information elements that may be used by multiple protocols, and the OUI field **618** may comprise a value suitable for identifying the information element as being utilized for setup. The configuration type field **620** may comprise 8 bits of binary information, for example, and may be vendor specific. The configuration subtype field **622** may comprise 8 bits of binary information, for example, and may be vendor specific. The version field **624** may comprise 8 bits of binary information, for example, and may comprise a value suitable for distinguishing different versions of the SP IE **612**. The data field **626** may comprise 8 bits of binary information, for example, to provide authorization enablement information that may be utilized by a client station that is being configured and authenticated utilizing a configuration protocol.

FIG. **6***c* is a diagram of an exemplary configuration protocol data field format, in accordance with an embodiment of the invention. With reference to FIG. **6***c* there is shown a configuration protocol data field **632**. The configuration protocol data field **632** may comprise a configuration protocol window open field **634**, a configuration protocol for wireless distribution system (WDS) window open field **636** and a reserved field **638** reserved for future use. The con-

figuration protocol window open field **634** may comprise 1 bit of binary information, for example, and may comprise information suitable for specifying a configurator timing window to a client station, such as, for example, client station **104**. The configuration protocol window open field **634** may be set to 1, for example, if the configuration protocol window is currently open for a configuration protocol client, for example, client station **104** and may be set to 0, for example, otherwise. The configuration protocol window open field **634** may indicate whether the configurator timing window is open, or closed. In this regard, the configuration protocol open window field **634** may specify a time period during which configuration is allowed. The configuration protocol for wireless distribution system (WDS) window open field **636** may be set to 1, for example, if the configuration protocol window is currently open for a configuration protocol WDS client and may be set to 0, for example, otherwise. The reserved field may comprise 6 bits of binary information, for example, and may be utilized for future use. The configurator, for example, AP **102** functioning as a configurator may indicate a recently configured state if none of the bits in the SP IE field **612** are set to 1, for example. The recently configured state may indicate whether the configurator has already configured another client during the current configuration protocol window opening period.

In operation, when the configurator timing window is open, a client, such as, for example, client station **104**, may be permitted to utilize a configurator, such as, for example, AP **102** functioning as a configurator station **102**, for configuration and authentication based on a configuration protocol. If the configurator timing window is closed, a client may not be permitted to utilize the configurator for configuration and authentication based on a configuration protocol. The amount of time that may transpire between when a configurator timing window is open and when the configurator timing window is subsequently closed may be determined during configuration of the configurator. If the client expected to be configured during the current configurator timing window but was unable to do so as a result of information in the recently configured field, the client may report that an unintended client may have utilized the configurator for configuration and authentication based on a configuration protocol.

FIG. **7***a* is a diagram of an exemplary configuration protocol packet header format, in accordance with an embodiment of the invention. With reference to FIG. **7***a*, there is shown configuration protocol packet header format **702**. The configuration protocol packet header **702** may comprise an Ethernet header field **724**, an extensible authentication protocol (EAP) header field **726**, a version field **728**, a configuration protocol type field **730**, a flags field **732** and a reserved field **734** for future use. The Ethernet header field **724** may comprise an Ethernet destination address and an Ethernet source address, for example. The EAP header field **726** may comprise data that specifies the version, type and length of the EAP header. The version field **728** may comprise information that identifies the version of the configuration protocol packet header **702**. The configuration protocol type field **730** may comprise information that identifies the packet type of the configuration protocol. The configuration protocol type field **730** may indicate a type of transmitted message between the configurator **208** and the client station **204**. For example, a hello message as illustrated in step **316**, a public key **1** message as illustrated in step **318**, a public key **2** message as illustrated in step **320**, a SSID/passphrase message as illustrated in step **322** or a status message **324**. The flags field **732** may comprise 8 bits of binary information, for example, and may be adapted to provide additional information pertaining to a configuration protocol at the configurator.

FIG. **7***b* is a diagram of an exemplary EAP header message format for a configuration protocol, in accordance with an embodiment of the invention. With reference to FIG. **7***b*, there is shown an EAP header **726**. The EAP header **726** may comprise a version field **754**, a packet type field **756**, a packet length field **758** and an EAP body field **760**. The version field **754** may comprise 8 bits of binary information, for example, that indicates the version of the extensible authentication protocol over LAN (EAPOL). The packet type field **756** may comprise 8 bits of binary information, for example, that indicates the type of the EAPOL packet utilized. The packet length field **758** may comprise 16 bits of binary information, for example, that indicates the length of the configuration protocol packet header **702**. The EAP header body field **760** may comprise data that indicates the EAP version, EAP type and EAP length of the configuration protocol packet header **702**.

FIG. **7***c* is a diagram of an exemplary EAP header body format for a configuration protocol, in accordance with an embodiment of the invention. With reference to FIG. **7***c*, there is shown an EAP header body field **760**. The EAP header body field **760** comprises an EAP code field **732**, an EAP ID field **734**, an EAP length field **736**, an EAP type field **737**, EAP vendor ID field **738** and an EAP vendor type field **739**. The EAP code field **732** may comprise information that indicates whether the EAP packet is a request identity packet or a response identity packet. For example, an access point **102** may communicate a request-identity EAP packet to the client station **104** to identify the client station trying to access the AP **102**. The client station **104** may respond by communicating a response-identity EAP packet to the AP **102** confirming its identity. The EAP ID field **734** may comprise information that indicates the current identity of the request-identity EAP packet. The EAP length field **736** may comprise information that indicates the length of the EAP header field **726**. The EAP type field **737** may comprise information that indicates the type of EAP packet. The EAP vendor ID field **738** may comprise 24 bits of binary information, for example, that indicates the vendor ID of the EAP packet. The EAP vendor type field **739** may comprise 32 bits of information, for example, that indicates the vendor type of the EAP packet.

FIG. **7***d* is a diagram illustrating an exemplary configuration protocol packet type key format, in accordance with an embodiment of the invention. With reference to FIG. **7***d*, there is shown a configuration protocol packet type key format **740**. The configuration protocol packet type key **740** comprises a configuration protocol header **702**, a public key length **744** and a public key **746**. The configuration protocol packet type key **1** and the configuration protocol packet type key **2** may have a format similar to the configuration protocol packet type key format **740**. The configuration protocol header **702** is substantially as described in FIG. **7***a*. The public key length field **744** may comprise information that indicates the length of the public key utilized. The public key field **746** may comprise algorithm information that specifies the public key **1** for the configuration protocol packet type key **1** or public key **2** for the configuration protocol packet type key **2**. For example, an encryption type may be specified during setup configuration and authorization of the client such as, for example, the Diffie-Hellman (DH) algorithm. The public key field **746** for the public key **1** message may comprise the configurator's generated public

key for algorithm information exchange, for example, DH algorithm information exchange. The public key field **746** for the public key **2** message may comprise the client's generated public key for algorithm information exchange, for example, DH algorithm information exchange. The client, for example, client station **104** may transmit a public key **2** message as illustrated in step **324** in response to a transmitted public key **1** message as illustrated in step **322** previously received from a configurator. The public key **2** message may be transmitted as plaintext.

FIG. **7***e* is a diagram illustrating an exemplary configuration protocol packet type info format, in accordance with an embodiment of the invention. With reference to FIG. **7***d*, there is shown configuration protocol packet type info format **750**. The configuration protocol packet type info format **780** comprises a configuration protocol header **702**, a service set identifier (SSID) field **784**, an encrypted passphrase field **786** and a passphrase length field **788**.

The SSID field **784** may comprise a unique identifier attached to the header of the configuration protocol packets sent over a WLAN that may act as a password when a client station, for example, client station **104** tries to connect to the BSS, for example, BSS **202**. The SSID field **784** may comprise information that indicates the SSID of the secure configuration protocol network. The SSID field **784** may specify an ESS, such as, for example, ESS **220**, to which the client may become a member. The encrypted passphrase field **786** may comprise information that is utilized to configure the client based on a configuration protocol. The encrypted pas sphrase field **786** may be randomly generated at the AP **102** and transmitted to the client **104** in an encrypted format. The key for the encryption may be derived using the Diffie-Hellman (DH) protocol or its variant, for example. The DH protocol may generate a shared 1536-bit key, for example. This key may be converted to a 128-bit key using an encryption algorithm such as secure has access 1 (SHA1), for example. The 128-bit key may be utilized for advanced encryption standard (AES) wrapping of the encrypted passphrase before being transmitted over the air. The encrypted passphrase field **786** may specify, as ciphertext, a secret key that may be utilized by the client to establish secure communications in an IEEE 802.11 WLAN. The encrypted passphrase field **786** may be decrypted based on the exchange of shared keys in the public key **1** message and the public key **2** message. The passphrase length field **788** may comprise information that indicates the length of the encrypted passphrase.

A configuration protocol packet type hello may be communicated from the client to the configurator to inform the configurator that the client is ready for exchange of packets. The configuration protocol packet type key **1** may be communicated by the configurator to the client in response to receiving the configuration protocol packet type hello from the client. The configuration protocol packet type key **2** may be communicated by the client to the configurator in response to receiving the configuration protocol packet type key **1** from the configurator. After the configuration protocol packet type key **1** and configuration protocol packet type key **2** have been exchanged, the configurator and client may calculate a shared secret key that may be utilized to encrypt the configuration information. The configuration protocol packet type info may be communicated by the configurator to the client in response to receiving the configuration protocol packet type key **2** from the client. The configuration protocol packet type status may be communicated by the client to the configurator in response to receiving the configuration protocol packet type info from the configurator. The configuration protocol packet type status may indicate the status of exchange of the configuration protocol messages. If the client successfully receives and decrypts the configuration information in the configuration protocol packet type info message, the client may communicate a configuration protocol packet type status message indicating a success of exchange of messages.

If the client did not receive the configuration protocol packet type info or is unable to decrypt the configuration information in the configuration protocol packet type info message, the client may communicate a configuration protocol packet type status message indicating a failure of exchange of messages. The configuration protocol packet type status may be communicated by the configurator **208** or the client station **204** at anytime to terminate the exchange of messages between the configurator **208** and the client station **204**, if required. A configuration protocol packet type echo request may be communicated by the client to the configurator during link verification and wired discovery. A configuration protocol packet type echo response may be communicated by the configurator to the client during link verification and wired discovery in response to a received configuration protocol packet type echo request from the client. The configuration protocol exchange is substantially as described in FIG. **3**.

Certain aspects of a method and system for enabling exchange of information in a secure communication system may comprise at least one configuration processor, for example, configuration processor **230** that uses authentication enablement information comprising data that specifies a time period during which configuration of at least one 802.11 client station, for example, client station **204** is allowed. The data that specifies a time period during which configuration is allowed may comprise a configuration protocol window open field **634**, which indicates a period when a configuration setup window is open. At least one client station, for example, client station **204** may be configured via the authentication enablement information comprising recently configured data, which indicates whether at least one configurator has configured at least one other client station within the time period during which the configuration is allowed.

The authentication enablement information may comprise recently configured data for configuring the client station **204**, which indicates whether the configurator **208** has configured at least one other client station, for example, client station **206** during the configuration setup window opening period. The configuration of the client station **204** may be disallowed if the recently configured data indicates configuration of at least one other client station, for example, client station **206** by the configurator **208** within the time period during which the configuration is allowed. The authentication enablement information may comprise at least one version field, for example, version field **624**, which indicates a version of a configuration protocol that is utilized to configure the client station **204**.

The configuration protocol version field **624** may comprise 6 bits of binary information, for example, and may comprise information suitable for distinguishing different versions of a configuration protocol. The configuration protocol window open field **634** may comprise 1 bit of binary information, for example, and may comprise information suitable for specifying a configurator timing window to a client station, such as, for example, client station **104**. The configuration protocol window open field **634** may indicate whether the configurator timing window is open, or closed. The authentication enablement information may further comprise an encrypted passphrase, for example, the encrypted passphrase field **786**, which authenticates the

802.11 client station **204**. The encrypted passphrase field **786** may be generated by an encryption algorithm, for example, the Diffie-Hellman (DH) algorithm. The public key field **746** for the public key **1** message may comprise the configurator's generated public key for algorithm information exchange, for example, DH algorithm information exchange. The public key field **746** for the public key **2** message may comprise the client's generated public key for algorithm information exchange, for example, DH algorithm information exchange. The client, for example, client station **104** may transmit a public key **2** message as illustrated in step **324** in response to a transmitted public key **1** message as illustrated in step **322** previously received from a configurator. The public key **2** message may be transmitted as plaintext.

The authentication enablement information may further comprise at least one service identifier, for example the SSID field **784**, which identifies the 802.11 client station **204**. The configuration processor **230** may be adapted to authenticate the 802.11 client station **204** via the authentication enablement information by exchanging a plurality of public keys. The authentication enablement information may further comprise status data, which indicates a status of messages exchanged between at least one configurator, for example, configurator **208** and at least one 802.11 client station, for example, client station **204**.

Accordingly, the present invention may be realized in hardware, software, or a combination of hardware and software. The present invention may be realized in a centralized fashion in at least one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system or other apparatus adapted for carrying out the methods described herein is suited. A typical combination of hardware and software may be a general-purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein.

The present invention may also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which when loaded in a computer system is able to carry out these methods. Computer program in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following: a) conversion to another language, code or notation; b) reproduction in a different material form.

While the present invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the present invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the present invention without departing from its scope. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed, but that the present invention will include all embodiments falling within the scope of the appended claims.

What is claimed is:

1. A configurator station comprising:

a configuration processor;

persistent memory coupled to the configuration processor and configured to store configuration information pertaining to previously configured client stations;

a button capable of being activated, wherein a time duration for which the button is activated corresponds to a first-duration button activation or a second-duration button activation;

the configuration processor configured to open a configurator timing window in response to the first-duration button activation; and

the configuration processor configured to release, from the persistent memory, the configuration information pertaining to previously configured client stations in response to the second-duration button activation.

2. The configurator station of claim **1**, wherein the configuration processor is further configured to generate either, or both of, a new Service Set Identifier (SSID) and a new passphrase in response to the second duration button activation.

3. The configurator station of claim **1**, wherein:

the first-duration button activation corresponds to one of a short button activation and a long button activation; and

the second-duration button activation corresponds to the other one of the short button activation and the long button activation.

4. The configurator station of claim **1**, wherein a length of time the configurator timing window remains open is configurable.

5. The configurator station of claim **1**, wherein the configuration processor is further configured to:

generate a first beacon frame including authentication enablement information to be transmitted during a time interval when the configurator timing window is open; and

generate a second beacon frame that does not include authentication enablement information to be transmitted during a time interval when the configuration timing window is closed.

6. The configurator station of claim **5**, wherein the authentication enablement information includes a flag indicating whether a client station has been configured during a current configurator timing window.

7. The configurator station of claim **6**, wherein the configuration processor is further configured to disallow configuration of more than one client station during the current configurator timing window.

8. A collocated device functioning as a configurator, the collocated device comprising:

a processor;

non-volatile memory coupled to the processor;

a button capable of being activated, wherein a time duration for which the button is activated corresponds to a short button activation or a long button activation;

during a time when the collocated device is an unconfigured collocated device, the processor initiates configuration of the collocated device in response to the short button activation; and

after the collocated device is configured, the processor opens a configurator timing window in response to the short button activation.

9. The collocated device of claim **8**, wherein the processor releases configuration information pertaining to previously configured client stations in response to the long button activation.

10. The collocated device of claim **8**, wherein the configuration includes obtaining either or both of a Service Set Identifier (SSID) and a passphrase to subsequently be utilized when configuring client stations.

11. The collocated device of claim 10, wherein the processor is further configured to obtain either or both of the SSID and the passphrase using manual entry.

12. The collocated device of claim 10, wherein the processor is further configured to generate either or both of the SSID and the passphrase.

13. The collocated device of claim 8, wherein the processor is further configured to:

generate a first beacon frame including authentication enablement information to be transmitted during a time interval when the configurator timing window is open; and

generate a second beacon frame that does not include authentication enablement information to be transmitted during a time interval when the configuration timing window is closed.

14. The collocated device of claim 13, wherein the authentication enablement information includes a flag indicating whether a client station has been configured during a current configurator timing window.

15. The collocated device of claim 14, wherein the configuration processor is further configured to disallow configuration of more than one client station during the current configurator timing window.

16. A system comprising:

a wireless access point;

a configurator collocated with the wireless access point, the configurator comprising:

a configuration processor;

memory coupled to the configuration processor and configured to store configuration information pertaining to previously configured client stations;

a button capable of being activated, wherein a time duration for which the button is activated corresponds to a first-duration button activation or a second-duration button activation;

in response to the first-duration button activation during a time when the configurator has been configured, the processor opens a configurator timing window; and

in response to the second-duration button activation, the processor forces previously configured client stations to repeat an authentication process to regain an ability to engage in secure wireless communications.

17. The system of claim 16, wherein the processor, in response to the second-duration button activation, releases the configuration information pertaining to previously configured client stations from the memory.

18. The system of claim 17, wherein the processor obtains either, or both of, a new Service Set Identifier (SSID) and a new passphrase in response to the second duration button activation.

19. The system of claim 16, wherein in response to the first-duration button activation during a time when the configurator is unconfigured, the processor initiates configuration of the configurator in response to the short button activation.

20. The system of claim 16, wherein the processor is further configured to:

generate a first beacon frame including a flag indicating whether a client station has been configured during a current configurator timing window; and

if the flag indicates that a first client station has been configured, disallow configuration of a second client station during the current configurator timing window.

* * * * *